ACCESS CONTROL FOR PORTABLE DATA STORAGE MEDIA

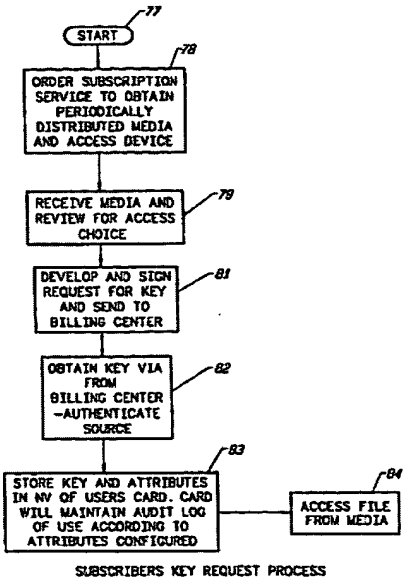
Publication number: JP9503322T
Publication date: 1997-03-31
Inventor:
Applicant:
Classification:
- international: ***G06F1/00; G06F12/14; G06F13/00; G06F21/00; G06F21/22; G06F21/24; G06Q10/00; G06Q30/00; G06Q50/00; G09C1/00; G11B20/10; H04H1/02; H04L9/32;*** **G06F1/00; G06F12/14; G06F13/00; G06F21/00; G06F21/22; G06Q10/00; G06Q30/00; G06Q50/00; G09C1/00; G11B20/10; H04H1/02; H04L9/32;** (IPC1-7): G06F1/00; G06F9/06; G06F12/14; G06F13/00; G06F17/60; G09C1/00; G11B20/10; H04H1/02; H04L9/32
- european: G06F21/00N7D; G06F12/14B
Application number: JP19940509362T 19940914
Priority number(s): WO1994US10455 19940914; US19930122005 19930914

Also published as:
WO9508231 (A1)
EP0719485 (A1)
EP0719485 (A4)
EP0719485 (A0)
EP0719485 (B1)
more >>

Report a data error here

Abstract not available for JP9503322T
Abstract of corresponding document: **WO9508231**

The system and method of the present invention provides the support of high density removable media (84), such as CD-ROM or MO, tobe used as distributed media for storing data where access thereto is securely restricted. Through this system and method, the secure periodic distribution of several different sets of data information (78) to the end user is achieved with access control selectively performed by at the user's site through communication with the billing/access center (81 & 82). User billing is based on the purchase of the decryption access codes (81 & 82) as indicated by the access code attributes encoded on the media (84). Access code availability if further controlled by selectively providing for updates of decryption access codes.



SUBSCRIBERS KEY REQUEST PROCESS

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平9－503322

(43)公表日　平成９年(1997)３月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		
Ｇ０６Ｆ	1/00	３７０	9469－5E	Ｇ０６Ｆ	1/00	３７０Ｆ
	9/06	５５０	9367－5B		9/06	５５０Ａ
	12/14	３２０	7623－5B		12/14	３２０Ｂ
	13/00	３５１	9460－5E		13/00	３５１Ｅ
	17/60		7259－5J	Ｇ０９Ｃ	1/00	６４０Ｚ

審査請求　未請求　予備審査請求　有　（全 42 頁）　最終頁に続く

(21)出願番号　特願平7－509362
(86)(22)出願日　平成６年(1994)９月14日
(85)翻訳文提出日　平成８年(1996)３月14日
(86)国際出願番号　ＰＣＴ／ＵＳ９４／１０４５５
(87)国際公開番号　ＷＯ９５／０８２３１
(87)国際公開日　平成７年(1995)３月23日
(31)優先権主張番号　０８／１２２，００５
(32)優先日　1993年９月14日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　スピラス　インコーポレイテッド
アメリカ合衆国　カリフォルニア州　95134　サンノゼ　ジャンクション　アヴェニュー　2841　スイート　110
(72)発明者　ドルフィン　ジャネット　リン
アメリカ合衆国　カリフォルニア州　95035　ミルピタス　カリスバッド　ストリート　602
(74)代理人　弁理士　杉村　暁秀　（外１名）

最終頁に続く

(54)【発明の名称】　小型データ記憶媒体に対するアクセス制御

(57)【要約】
本発明のシステムおよび方法は、データを記憶し、このデータへのアクセスが安全に制限された流通媒体として使用すべき、ＣＤ－ＲＯＭまたはＭＯのような高密度リムーバブル媒体のサポート（８４）を提供する。このシステムおよび方法によって、エンドユーザへのデータ情報のいくつかの異なった組の安全な定期的な流通（７８）が、ユーザのサイトにおける課金／アクセスセンタとの通信（８１および８２）によって選択的に行われるアクセス制御によって達成される。ユーザの課金は、前期媒体において符号化されたアクセス符号属性によって示される復号化アクセス符号の購入に基づく。アクセス符号の有効性を、復号化アクセス符号の更新を選択的に行うことによって、さらに制御する。

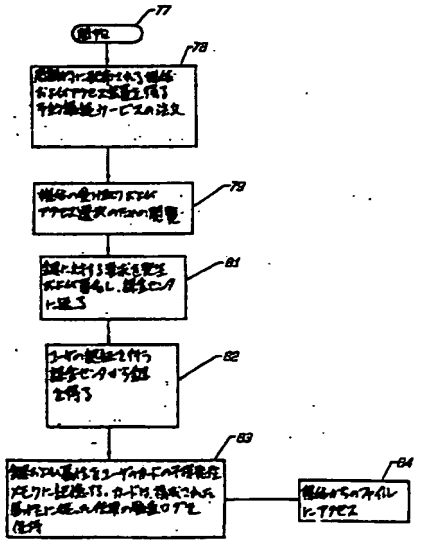


FIG. 13

【特許請求の範囲】

1．ユーザによってデータにアクセスするシステムであって、

データを処理するプロセッサと、

前記データを記憶するデータ記憶ユニットであって、前記記憶ユニットに記憶された対応する異なったデータにアクセスするために異なったアクセス符号を要求するデータ記憶ユニットと、

前記プロセッサと通信し、遠隔地から前記異なったアクセス符号の1つを表す信号を受け、前記アクセス符号の1つを使用する前記データ記憶ユニットにおける前期データの選択された部分への前記プロセッサ手段によるアクセスを可能にする信号を送るコントローラと、

前記プロセッサおよび前記コントローラから離れた場所に位置する遠隔許可ユニットであって、前記ユーザによって前記遠隔許可ユニットに送られた許可要求信号に応じてアクセス符号を前記離れた場所から前記コントローラに伝送する遠隔許可ユニットとを具えるシステムにおいて、

前記データ記憶ユニットが、前記伝送されたアクセス符号と協調し、電子更新カウンタの状態が一致した場合、前記データ記憶ユニットの以前アクセスできなかった部分にアクセスするための更新アクセス符号を自動的に発生する更新手段を格納することを特徴とするシステム。

2．データをユーザに流通させる方法において、

記憶ユニットにおいて、暗号化データを供給し、前記データへのアクセスを与えるために前記データを復号化するアクセス符号を要求し、前記暗号化データの小さい部分を、アクセス符号を識別する対応するアクセス識別子に関係させるステップと、

遠隔地において、複数のアクセス符号を、対応するアクセス符号識別子と共に記憶するステップと、

遠隔値において、個々の状態が一致した場合、許可信号を発生し、前記許可信号が、前記アクセス符号の1つを前記ユーザに伝送させ、前記暗号化データの一部を復号化することによって、前記ユーザが前記暗号化データの一部にア

クセスできるようにし、前記アクセス状態が、前記ユーザから前記アクセス符号識別子の一つを受け取ることを含むステップと、

前記アクセス符号を前記暗号化データに用い、前記暗号化データの一部を復号化するステップと、

前記暗号化データの前記復号化部分を処理するステップとを具える方法。

3．データセットの形式の情報を流通させ、この情報へのアクセスを与える方法において、

前記データセットを暗号化し、前記データセットの異なった部分を復号化するために異なったアクセス符号が必要となるようにするステップと、

前記データセットを、前記データセットを復号化する個々のアクセス符号を識別するアクセス符号識別子と関係させるステップと、

前記データセットをデータ記憶ユニットに書き込むステップと、

前記アクセス符号を前記データ記憶手段に用いることができるデータ記憶コントローラを設けるステップと、

データアクセスコントローラを前記異なったアクセス符号の１つに遠隔的に用い、前記アクセス符号識別子の受け取りに応じて、前記暗号化データセットの選択された１つを復号化するステップと、

前データアクセスコントローラが、前記データ記憶手段に書き込まれた前記データセットにアクセスするステップと、

前記アクセス符号を、前記データセットの個々の特性に対応するように規定された属性と共に記憶し、これらの双方を、前記アクセス符号識別子の１つの受け取りに応じて前記データアクセスコントローラに伝送するステップとを具える方法。

4．個々のデータセットを暗号化し、アクセス符号識別子を前記個々のデータセットに割り当てるプログラミング符号を含み、前記個々のアクセス符号を識別する前記アクセス符号識別子の各々が、前記個々のデータセットの１つを復号化する個々のアクセス符号と関連し、これを復号化するのに使用されるメモリ媒体と、

前記メモリ媒体と通信し、前記暗号化された個々のデータセットをデータ記

憶ユニットに記憶し、前記データセットの少なくともいくつかを、前記データ記憶ユニットにおけるアクセス符号識別子と関連して記憶するようにするプロセッサと、

前記アクセス符号識別子の１つの受け取りにおいて、前記データ記憶ユニットに使用するために、前記アクセス符号のある１つを伝送するリモートアクセス符号流通コントローラとを具える、データを暗号化するシステム。

５．前記データセットの個々の特性に対応するように属性を規定するステップと、

前記属性をアクセス符号に結合し、これらを第１の場所において記憶するステップと、

前記アクセス符号が前記データセットにプロセッサによって用いられた場合、前記アクセス符号によって復号化できるように前記データセットを符号化するステップと、

前記符号化されたデータセットをデータ記憶ユニットに記憶するステップと、

前記属性の１つに結合された前記アクセス符号の１つを前記第１の場所から第２の場所に伝送するステップとを具える、データセットを暗号化し、これらへのアクセスを制御する方法。

６．ユーザによって選択された部分を含むデータを含むデータ記憶ユニットを具え、前記データ記憶ユニットにおける前記選択された部分が、アクセス符号の組によってアクセス可能であり、前記アクセス符号の組の１つを遠隔中央処理ユニットによって異なった場所におけるユーザに伝送し、前記ユーザに伝送された前記アクセス符号が、前記データ記憶ユニットに記憶された前記データの前記選択された部分へのアクセスを与える、ユーザによって使用されるデータ検索システムにおいて、

前記データ記憶ユニットが、電子更新カウンタの状態が一致した場合、前記伝送されたアクセス符号と協調し、前記データ記憶ユニットにおける前記データの前記選択された部分の以前アクセスできなかった部分にアクセスするための更新アクセス符号を自動的に発生する更新手段を含むことを特徴とするシス

テム。

【発明の詳細な説明】

小型データ記憶媒体に対するアクセス制御

技術分野

本発明は、小型データ記憶ユニットにおいて記憶されたデータへのアクセスを提供することに関する。さらに特に、本発明は、暗号化されたデータを小型データ記憶ユニットにおいて供給し、遠隔地からアクセス符号を送信し、前記暗号化されたデータを復号化するシステムに関する。

背景技術

データ高密度記憶技術の進歩が進み続けているため、多くの家庭および企業が、新たな形態の小型データ記憶媒体を読み取ることができるコンピュータ周辺装置を取得している。例えば、コンパクトディスク－読み出し専用メモリ（ＣＤ－ＲＯＭ）のような高密度媒体が、テキスト、ビジュアル（ビデオまたは写真）およびオーディオ情報に加えてインタラクティブメディアのような、進歩した形態の電子情報を記憶する安価な媒体になってきている。ＣＤ－ＲＯＭは、２５００００ページのテキスト、１２０００の画像、１．５時間のビデオ、５００冊のペーパバック、または４３０冊の雑誌に相当するデータを保持するのに十分な記憶空間を含む。さらにＣＤ－ＲＯＭ技術は、複製されたＣＤ当たり平均０．０５ドルという極めて高い費用効果的な複製の特徴を持っている。ＣＤ－ＲＯＭプレイヤを、テレビジョン受像機またはコンピュータに結合し、ユーザが、ＣＤ－ＲＯＭに記憶されたテキストまたはビジュアル情報に加えてオーディオ情報にアクセスできるようにすることができる。

大部分の出版業者にとって共通の習慣は、ワードプロセッサおよびコンピュータにおいて、彼らの情報を電子的に収集し、処理することである。これらのデータは、購読者に郵送される時まで、電子的形態で保持される。郵送する時、この情報は印刷され、購読者郵送ラベルが貼られ、出版された情報は、郵送サービスを経て講読者に送られる。このシステムの下で、印刷および配送の費用は、極めて高い。さらに、環境への関心が、紙を不足する資源として考える必要性を強いている。したがって、新たな出版媒体の必要性が認識されている。例えば、１９

８９年５月２日、１９９０年１０月１１日および１９９１年９月１７日に各々Ｓｈｅａｒに対して発行された米国特許第４８２７５０８号、４９７７５９４号および５０５０２１３号を参照されたい。

標準的な郵便手段による家庭およびオフィスへの予約講読サービスは、雑誌、業界紙、金融最新情報、および月毎の本を購読者に提供する。これらの予約講読サービスは、ユーザ（購読者）に、一定の金額を予めまたは月毎に支払うことを要求する。予約講読が有効な間、出版業者は、その情報を購読者に郵送し続ける。さらに、どの一人のユーザも、多数の業界紙または雑誌の購読者かもしれない。また、一人のユーザは、同じ出版業者によって出版されたいくつかの雑誌に対する予約講読を続けるかもしれない。

団体、政府または法律の記録のような他の形式の出版または公的記録された情報も、広めるために紙に印刷される。このような広められた記録が、読むことを許可されない読み手によって偶然にまたは故意に読まれるかもしれない場合、この読み手が印刷物へのアクセスを許可されることから守る手段はない。さらに、ある出版された団体または法律情報は、以前出版された題材を時代後れにする頻繁な更新を受けるため、古くなった題材を流通から取り除くことは、望ましいが、しばしば困難である。

再びＳｈｅａｒ特許を参照すると、これらのシステムは、ユーザのアクセス活動度を、検査または測定する。暗号化データを開ける鍵は、ＰＣＭＣＩＡカードのようなユーザのハードウエアに存在するため、データに対する許可されていないアクセスを防ぐために、ユーザ側における復号化機能は禁止される。したがって、Ｓｈｅａｒのシステムによれば、ユーザは、ＣＤ－ＲＯＭのような小型記憶媒体における情報へのアクセスを、アクセスに対する先立った許可なく利用できる。したがって、読み手が、ユーザのアクセスの前にＣＤ－ＲＯＭに記憶された情報へのアクセスを許可されるのを保証する方法はない。さらに、これらのシステムは、古くなった情報へのアクセスを制限できる方法を提供しない。

例えばＣＤ－ＲＯＭに記憶された情報を、許可されていないアクセスから防御する必要性は、このような出版配布システムが、出版業者に受け入れられる前に

、満足される必要がある。出版業者側および購読者側の双方に設けられた防御手段が、媒体に含まれるデータへの許可されていないアクセスを防ぐために必要である。さらに、正当な購読者を、彼らの予約講読サービスが終了した場合、防御するようにする必要がある。

発明の開示

本発明には、少なくとも３つの基本的な特徴がある。これらは、個々の方法におけるデータの暗号化と、個々の流通機構の下での前記データの復号化と、更新機構による前記データの使用の制御とを含む。これらの基本的な特徴によって、以下に詳述するような多くの利益が提供される。

本発明は、好適には高密度で、ＣＤ－ＲＯＭまたは光磁気（ＭＯ）のようなリムーバブルまたは小型媒体においてデータを出版することを含む。したがって、１つまたはそれ以上の出版業者が、彼らの定期的な出版のすべてではないにしてもいくつかを、１つの媒体に編入することができる。本発明は、異なった出版物によって前記媒体をデータセットに分割し、これらのデータセットに対する保護、アクセスおよび使用監査機構を設けることを含む。したがって、確認された購読者のみが、ＣＤ－ＲＯＭに記憶された情報へのアクセスを得ることができる。

本発明の他の重要な特徴は、データを構成および設定し、出版業者自身の選択によって課金する道具を出版業者に提供することである。媒体を製造する時、出版業者は、販売している情報の形式に応じた購読者への課金に柔軟性を持たせる。この柔軟性を、出版処理に結合する。

さらに特に、本発明の前記保護およびアクセス機構は、例えば人格化されたＰＣＭＣＩＡまたは他の好適なプログラム記憶媒体における暗号化道具を、出版業者に提供することを含む。本発明のこの実現に従って、出版業者が局所的に記憶されたプログラムをロードした場合、オプションメニューが出版業者のコンピュータ画面上に現れ、出版業者に出版業者のデータへのユーザまたは購読者のアクセスを規定させる。課金オプションは、「属性」としても知られており、例えば、予約講読期間を含む。課金属性を、鍵材料識別子（Key Material Identifiers：ＫＭＩＤ）に関連付け、この識別子は、本質的に、課金属性をアクセス符号に

関連させる目的のインデックスまたは識別コードである。アクセス符号および鍵を、ここでは交換可能として使用する。ＣＤ－ＲＯＭに記憶されたデータの個々のセグメントに対応するアクセス符号を、最後に購読者にダウンロードし、購読者が前記情報へのアクセスを得られるようにする。

出版業者のＰＣＭＣＩＡに記憶されたプログラムは、出版業者がデータを暗号化し、それを復号化するためにアクセス符号または鍵が必要となるようにすることができるようにする。次にＫＭＩＤを伴った暗号化またはスクランブル化データを、小型記憶媒体に記憶する。対応する課金情報も、ユーザのレビュー用の別個のファイルに記憶する。次にこのＣＤ－ＲＯＭを、ユーザに送る。ユーザも、課金／アクセスセンタと連絡するとともにダウンロードされたアクセス符号を処理するソフトウエアを有するＰＣＭＣＩＡまたは他の好適な記憶媒体を所有している。さらにユーザは、電話線又はそれに比すべき媒体と、モデムを有するコンピュータと、ＰＣＭＣＩＡおよびＣＤ－ＲＯＭを読み取ることができる周辺装置とを有する。

ユーザのパーソナルコンピュータにおけるアプリケーションは、ユーザが、出版業者のデータを含むＣＤ－ＲＯＭを、読み取りハードウエアにロードした場合、コンピュータの画面上にメニューが現れるようにすることができる。このメニューは、例えば、売り物の出版物および課金情報を載せる。次にユーザは、ＰＣＭＣＩＡカードに記憶されたソフトウエアによって、売り物の出版物を強調または指示し、次に課金／アクセスセンタに要求を送ることによって、１つまたはそれ以上の出版物へのアクセスを要求する。ＫＭＩＤまたは識別インデックスと、クレジットまたはクレジットカード番号のような要求された課金データとを、遠隔地の課金局に電話線を経て送る。課金局は、クレジットの承認によって、ＫＭＩＤをアクセス符号に一致させ、鍵と、例えば購入された定期講読の期間であるアクセスパラメータとを、ユーザに電話線を経て伝える。次に鍵を、ユーザのＰＣＭＣＩＡカードにインストールする。次にユーザは、個々のアクセス符号または鍵によってアクセスできる個々の出版物にアクセスすることができる。

図面の簡単な説明

図１は、本発明による全体のシステムを示す。

図２は、図１の囲み１１のユーザ／課金局を示す。

図３は、図１の囲み１２の出版業者／課金局を示す。

図４は、出版業者およびユーザによって課金／アクセスセンタに送られる情報を図式的に示す。

図５は、本発明による出版業者局のいくつかの要素のブロック図である。

図６は、出版業者のＰＣＭＣＩＡのブロック図である。

図７は、出版業者の課金ソフトウエアのフローチャートである。

図８は、本発明による出版業者の使用中に利用できる属性選択の画面表示を示す。

図９は、本発明による出版業者の使用中に利用できるセキュリティ選択の画面表示を示す。

図１０は、本発明によるリムーバブル媒体に記憶される情報の形式のリストを示す。

図１１は、本発明による出版業者局のいくつかの要素のブロック図である。

図１２は、出版業者のＰＣＭＣＩＡのブロック図である。

図１３は、出版業者の鍵要求処理のフローチャートである。

図１４は、鍵データベースおよび課金／アクセスセンタのブロック図である。

図１５は、課金／アクセスセンタ処理のフローチャートである。

図１６は、本発明による暗号化更新特徴を説明する図である。

本発明の詳細な説明

本発明によるシステムおよび方法は一般に、２つのサブシステムおよびサブ方法を含む。この記述の第１の部分を、これらの２つのサブシステムと、システム全体を形成するためにこれらのサブシステムをどのように相互に関係させるかとに焦点を合わせる。以下に始めるこの記述の第２の部分を、本システムの各々の部分の実現に集中する。

図１を参照すると、囲み１１および１２は、囲み１３において重なった、全体のシステムの別個の部分である。囲み１２において、データの出版業者２１を示

す。このデータは、以下にＣＤ－ＲＯＭ２２と称するような小型記憶ユニット２２に記憶できるようなどの様な形式のデータも含むことができる。データを発生した後で、かつＣＤ－ＲＯＭ２２に記憶する前に、適切なアクセス符号なしでアクセスできないように、暗号化またはスクランブル化をする。したがって本発明は、対称鍵暗号化、ディジタル署名、非対称鍵交換、または請求応答のような、標準的な暗号化技術を取り入れる。代わりに、本発明は、どのような非標準的な暗号化技術を使用してもよい。

出版業者２１は、データを符号化した後、以下に詳細に記述するように、課金／アクセスセンタ２３に特定の情報を伝える。出版業者２１は、暗号化データをＣＤ－ＲＯＭ２２に記憶し、次にこのデータを、郵便サービスのような配達チャネルを経て配達する。配達チャネルは、例えば、特に団体、政府または法律の環境におけるオフィス内配達を含むことができる。最後に、ＣＤ－ＲＯＭは、ユーザ２６によって受け取られる。ユーザは、コンピュータ（プロセッサを含む）か、プロセッサおよびＣＤ－ＲＯＭ読み取り器を有するテレビジョン受像機またはモニタを有する。ユーザのコンピュータに、課金／アクセスセンタ２３との通信に使用し、課金／アクセスセンタ２３から受けたデータを処理するコントローラを有するソフトウエアプログラムおよび／またはハードウエアを設ける。

ユーザ２６が、ＣＤ－ＲＯＭ２２をＣＤ－ＲＯＭ読み取り器にロードした場合、ユーザは、どのようなデータがＣＤ－ＲＯＭ２２に記憶されているかを示す、コンピュータまたはテレビジョンモニタまたは画面上のメニューを提示される。ＣＤ－ＲＯＭ２２のデータの一部を、ユーザがアクセス符号なしにこの部分にアクセスできるように、暗号化しなくてもよい。しかしながら、本発明によれば、データの少なくとも一部を暗号化する。ユーザが暗号化データにアクセスするために、ユーザは、アクセス符号または鍵を手に入れ、暗号化データを復号化しなければならない。アクセス符号を得るために、ユーザ２６は、課金／アクセスセンタ２３と、電話線か、他の通信装置または仕掛けを経て通信し、個々のアクセス符号に対する要求を送る。許可された後、課金／アクセスセンタ２３は、ユーザ２６に接続部２７を経て、データを復号化するアクセス符号を、ダウンロード

または送信する。

図２は、ユーザ／課金／アクセスセンタサブシステムを詳細に示す。上述したように、ユーザのコンピュータに、課金／アクセスセンタ２３との通信に使用し、課金／アクセスセンタ２３から受けたデータの制御に使用するソフトウエアプログラムおよび／またはハードウエアを設ける。図２に示すように、「画面」を開き使用する準備をするアプリケーションを、計算機に常駐させる。したがって、ＰＣＭＣＩＡドライブ３２にロードされたＰＣＭＣＩＡカード２９と、ユーザが操作しているコンピュータ３１との間の通信が可能になる。ＰＣＭＣＩＡカード２９をユーザに供給し、ユーザが、暗号化データを復号化するアクセス符号に関する要求を、課金／アクセスセンタ２３に供給できるようにする。許可された後、課金／アクセスセンタ２３は、ユーザ２６にアクセス符号を接続部２７″を経てダウンロードまたは送信する。接続部２７′および２７″を、標準電子メールフォーマットを含むような、同じラインまたは伝送手段とすることができる。アクセス符号または鍵を、以下に明らかにするような理由のため、ユーザのＰＣＭＣＩＡカード２９に記憶する。

ここで図３を参照すると、出版業者局３６は、情報を編成し蓄積するワークステーションから成る。ＣＤ－ＲＯＭを製造する書き込み装置３５は、出版業者のワークステーションと連絡する。出版業者に、自分自身の出版業者ＰＣＭＣＩＡカード３３を供給し、このカードに、出版業者が、情報をＣＤ－ＲＯＭにおける出版物に編成したときに、データへのアクセスを規定および制御できるようにするために、ソフトウエアプログラムを記憶する。代わりに、ハードウエアを、出版業者にソフトウエアの代わりに供給してもよい。

上述したようなデータ３４は、例えば、ビデオ、画像、写真、データベース、音声、およびソフトウエアを含むことができる。このデータを、出版業者のコンピュータ３６において生成またはこれにダウンロードする。本発明にしたがって、データをＣＤ－ＲＯＭ２２に記憶する前に、出版業者は、例えば、個々の雑誌、個々のデータベース、同様の写真の組、実行可能なソフトウエアのモジュール、および個々のフォントである同様のデータに基づいて課金の配分を規定する。さらに出版業者は、データを、異なった対称暗号化鍵に属するファイル、サブデ

ィレクトリ、ディレクトリ、およびボリュームのような異なったデータセットに分割し、各々の異なったセグメントへのアクセスを、そのデータセグメントに一致する鍵によってのみ可能となるようにする。

課金の配分を、出版業者がデータのアクセスに対する請求をどの位にしたいかに従って、分類する。したがって、データセットへのアクセス制御を、本発明の課金または「属性」機構によって制御する。出版業者によってデータセットに属性を割り当て、この属性を、個々のデータセットを復号化するのにユーザによって使用されるような、以下に鍵と呼ぶアクセス符号に結合する。次に個々の対称鍵を、以下に詳細に記述する固有の鍵材料識別子（Key Material Identifiers：ＫＭＩＤ）に結合または割り当てる。

属性を、規定し、実行し、使用して、アクセスに先立って、ユーザ２６による暗号化されたデータへのアクセスの課金を決定する。この属性の一例は、継続期間である。例えば、あるＣＤ－ＲＯＭは、雑誌の１月号を含んでもよい。１月の後の月に発行されたＣＤ－ＲＯＭは、同じ雑誌のその後の号を含んでもよい。出版業者は、１年、２年および３年の予約講読の申込みとともに、自由な一ヵ月の試験講読の申込みを望んでもよい。これらの４つの異なった継続期間は、４つの異なった属性を構成する。したがって、本発明によれば、暗号化更新処理を使用し、ユーザによって選択された継続期間に応じて一定の期間アクセスできるようにすることができる。属性の構成を、距離があることを示すフラグと、距離値およびユニットを示すパラメータとを含む可変長のデータ構造とする。

属性の他の例は、情報が一度購入され、その鍵によって保護されている全ての情報が購読者によって利用可能である場合の「一度購入」属性を含む。鍵を使用できる回数、売買の総数、および転送されたバイト数またはファイル数を含む、出版業者が規定するパラメータに基づいて、データの使用を監視する「オンデマンド」属性も含む。さらに、このような属性を宣伝することができる。例えば、「ファイルバイパス」属性は、出版業者が、バイパスされるまたはプレーンテキスト中にあるファイルまたはデータセットを規定できるようにする。また、「試用期間」属性は、ユーザが、複製または印刷できずに、一定の期間これらのファイルへのアクセスを得られるようにすることができる。このような試用期間、ア

プリケーションは、ＰＣＭＣＩＡカードと直接通信し、複製または印刷のようなアプリケーションの特定の機能へのアクセスを制御する。これらのアプリケーションを、ＰＣＭＣＩＡインタフェースを支持するように変更する。さらに、「減少解像度」属性によって、出版業者は、特定のファイルの閲覧を、高解像度でなく行うことができる。これらの属性を、定数値によって表現できるものとすることができ、関数の変数とすることもできる。

出版業者によるデータ分割の決定の後、かつ、出版業者が各々のデータセットに使用されるべき属性を規定した後、属性を、鍵および鍵材料識別子（ＫＭＩＤ）に結合する。ＫＭＩＤは、識別符号として機能し、課金／アクセスセンタが、所望のデータセットを開ける適切な鍵またはアクセス符号を提供できるよにする。この情報を、出版業者によって結合し、流通すべき媒体全体に関する属性情報を含む固有ファイルを生成する。この情報を、課金／アクセスセンタに送る。さらにＰＣＭＣＩＡカードに記憶されたソフトウエアは、出版業者が、データを暗号化し、属性およびＫＭＩＤをＣＤに含められるようにする。

したがって本発明によるシステムは、鍵およびＫＭＩＤのデータベースへの割り当てと、これらの情報の課金／アクセスセンタ２３による保持とを含む。本システムは、所望のデータにアクセスする鍵を受け取るために、ユーザが、課金／アクセスセンタに特定のＫＭＩＤを送ることをさらに含む。本システムのこれらの要素を図４に示し、ここで、出版業者は、各々のデータセットのための鍵、属性およびＫＭＩＤを含む固有ファイル３７を、課金または許可センタ２３である課金／アクセスセンタ２３に伝送する。このファイル３７を、中央流通サイトにダウンロードする。ＣＤ－ＲＯＭ２２に書き込むのに必要な情報は、セクタの開始および終了情報と、各々のデータセット３８に関連するＫＭＩＤのみである。購読者が、個々のデータセットに対する（属性に調和する）値付けに関する情報を読めるようにする専用の「リードミー」ファイルを形成することができる。次に出版業者は、「マスタ」情報を複製し、なんらかの好適な輸送方法を経て流通させる。

図２に戻ると、ユーザ２６は、ＣＤ－ＲＯＭをＣＤ－ＲＯＭ読み取り器２８にロードし、専用の「リードミー」ファイルを読み、何が小型記憶媒体において利

用できるかを知ることができる。ユーザ２６が、アクセスしたいデータセットを識別した場合、ユーザ２６は、ＰＣＭＣＩＡドライブ３２にロードされたＰＣＭＣＩＡカード２９を使用し、課金／アクセスセンタ２３と通信し、所望の鍵を識別するＫＭＩＤを含む要求をライン２７′を経て送る。課金／アクセスセンタは、アクセスを許可すると、ライン２７″を経てＫＭＩＤに関係する鍵をダウンロードする。

ダウンロードの時、鍵を、ユーザのＰＣＭＣＩＡカード２９または適切なハードウエアに置いてもよい。鍵は、属性の制限に従って、流通されたすぐに使用できるＣＤ－ＲＯＭおよび次のＣＤ－ＲＯＭのデータセットにアクセスする。したがって、属性が、図４の囲み３７および囲み３８に示されているように６か月の継続期間を示し、最初のアクセスが１月に生じる場合、ユーザ２６は、後に流通されたＣＤ－ＲＯＭの同じデータセットにアクセスするために、６月までユーザＰＣＭＣＩＡカード２９を使用してもよい。鍵の最初の使用の後、キーのその後の使用は、ローカルユーザ環境によって、ユーザＰＣＭＣＩＡカード２９を通じて、継続され、監査される。

属性に継続期間制限を設けるために、本発明は、属性状態が満足された場合に生じる、または課金／アクセスセンタによって遠隔的に呼び出すことができる「鍵ゼロ化」を利用する。例えば、満足されている属性情報は、タイムクロックによって監視しうる時間経過を含む。更新されたデータは、周期的に発表されることから、鍵を、暗号化更新処理によって、初めに生成された鍵から得る。この特徴によって、出版業者は、暗号化操作に基づく最後の鍵から得た異なった鍵に属する周期的な情報を流通させることができる。購読者に対して有効な更新の回数を、ＫＭＩＤ／属性情報に符号化する。本発明の暗号化更新処理を、図１６の参照とともに以下に詳述する。

ユーザのＰＣＭＣＩＡカード２９を使用し、出版業者によって与えられた更新の計数を監査および保持する。各々のＣＤ－ＲＯＭは、個々のＫＭＩＤの更新発表についての情報と、鍵管理機能に基づく時間ユーザのＰＣＭＣＩＡカード２９によって使用されたタイムスタンピング情報とを含む。クロックを、ＰＣＭＣＩＡカードに取り付けてもよい。

本発明のゼロ化特徴は、頻繁に更新される例えば、団体、政府または法律の記録のアクセスを、回避または停止することができるという利点を提供する。データを１回だけまたは数回閲覧した後、または短期間の後、ゼロ化する鍵を使用することによって、出版社は、古くなった頻繁に更新された記録が、現在の記録と混同されないことを確実なものとする。

さらにユーザのＰＣＭＣＩＡカード２９を使用して、課金／アクセスセンタに対して購読者を認証する。各々の購読者を、ユーザのＰＣＭＣＩＡカード２９に記憶されているような、すべての伝送において使用すべき固有公開／非公開鍵対に割り当てる。異なったユーザの鍵対または人格は、ユーザが、個々の人格によって購入注文に署名すること、または購入要求を行うことを可能にする。この特徴は、一人の人間が、一時的にまたは常時いくつかの異なったオフィスを保持している状況において重要である。例えば、会社の社長が、別個の要求に、購入代理人として署名してもよく、別個のアクセス要求に、会社の社長として、異なった特権によって署名してもよい。したがって、本発明は、購読者によって規定される異なったユーザ人格の認証をサポートし、電子購入許可を提供する。さらに、各々のユーザＰＣＭＣＩＡカード２９は、ユーザおよび彼らの人格の使用と、ユーザのサイトにおけるカードの暗号化機能とを有効にする固有ピンフレーズを含む。

個人がＣＤ－ＲＯＭに記憶されたファイルへのアクセスを得ようとする場合、鍵は、すでに出版されているカードに常駐していなければならない。もしそうでないと、購読者は、購入要求を生成し、この要求を課金／アクセスセンタに送らなければならない。例えばクレジットカード番号である支払い方法を含むすべての要求を、公開／非公開鍵対に暗号化する。すべての購入要求を、課金／アクセスセンタがなんらかの購入要求を処理する前に、適切な権限を与える人格によって署名することもできる。

団体、政府または法律の情報を組織内で提供するオフィス内流通の場合である、購入がなされない状況において、認証特徴は、特に望ましい。変動しやすい情報に対する非認証アクセスは、情報が印刷媒体において配布される場合より、本発明にしたがってより容易に回避される。

再び図１を参照すると、課金／アクセスセンタ２３は、要求２７を、例えば電子メールの形式で受ける。このメールを受け取り、署名を確認し、要求元を認証する。メールに含まれるメッセージは、要求されたＫＭＩＤ（図４参照）である。次にこのＫＭＩＤを、記憶された暗号鍵を含む大きいデータベースへの検索見出しとして使用する。本発明の一実施例において、以下のステップが生じる。課金／アクセスセンタ２３は、ＫＭＩＤに割り当てられた出版業者によって規定された属性をデータベースから得て、この情報を要求者に提供する。次に要求者は、課金／アクセスセンタに送られる、鍵の支払いの形態を選択することができる。次に課金／アクセスセンタは、支払い方法を確認し、認証する。次にＫＭＩＤおよびこれに結合された属性を、ユーザに送る。ユーザのサイトにおいて、ＫＭＩＤおよび属性を、アクセスを制御および監査するユーザＰＣＭＣＩＡカード２９にロードする。ここでユーザは、購入された情報へのアクセスを有する。ＫＭＩＤと、出版業者の規定に従った鍵の使用を、ユーザのＰＣＭＣＩＡカード２９によって監視および保持する。上述したように、属性状態が一致した場合、例えば、購読者が購入バイト数に達した場合、または時間が満期になった場合、ユーザのＰＣＭＣＩＡカード２９は、この出版物に関しては自動的にゼロ化する。ユーザによるさらなるアクセスは、課金／アクセスセンタ２３への他の呼出しを必要とする。

上記の説明は、本発明によるサブシステムの一般的な特徴と、これらが互いにどのように関係するかを詳細に記述した。下記の説明は、本発明の素子の相互関係をより強調せず、本発明の部品および方法ステップをより強調して、上記の説明をある程度繰り返す。

上述したように、出版業者の情報を論理的に組分けおよび分類することによって、出版業者は、出版すべき情報セットに関連する課金および広告機能を規定することができる。出版業者が、１枚のＣＤ－ＲＯＭまたは１組のＣＤ－ＲＯＭにおける出版物に使用とする全ての情報を集めた後、この情報に、本発明によって規定されるアクセスおよび予約講読属性を割り当てる。標準的な出版業者の形態を、図５のブロック図において示す。情報の収集および編成を行う出版業者のワークステーション３６を示す。出版業者に、このような編成のための課金前マス

タリングソフトウエア４１を提供する。ＣＤ－ＲＯＭライタドライバ３５は、ワークステーションと連絡して、ＣＤ－ＲＯＭを生成する。最後に、出版業者のサイトに記憶された鍵データベース４２は、使用された鍵およびそれらの別名と、履歴と、現在の属性規定とを含む。鍵データベース４２は、出版業者が使用することができ、属性を規定することができる使用されていない鍵のリストも含む。出版業者が個々の鍵の使用を決定した後、この情報を遠隔地の課金／アクセスセンタ２３に送る。

暗号化装置４３を、図６に示す出版業者のＰＣＭＣＩＡカード３３に格納する。各々の出版業者を、フラッシュまたはＥＥＰＲＯＭ不揮発性メモリ４４に中に出版業者の人格を含み、出版されたデータとその著者についての監査情報を提供する唯一の個人的なＰＣＭＣＩＡカード３３に割り当てる。出版業者の人格は、上述したユーザの人格と同様のものである。さらに不揮発性メモリ４４は、パスワードアルゴリズムの一部として使用される出版業者の固有記憶変数（K_S）を含む。前記の情報を、出版業者のＰＣＭＣＩＡカードに記憶し、この局所鍵によって暗号化することができる。加えて、出版業者のワークステーションは、個々のＣＤ－ＲＯＭの出版に使用されたＣＤ－ＲＯＭ識別子およびＫＭＩＤを自動的に記録する。この監査データを、鍵データベース４２によって記憶し、保持する。

ＰＣＭＣＩＡカード３３によって供給されたディジタル署名は、出版されたデータが、個々の情報の許可された出版業者によってＣＤ－ＲＯＭにおいて出版されたことを、課金／アクセスセンタおよび／または購読者に対して保証する。この特徴は、版権を取得した材料の著作権侵害に加え、団体、政府または法律の環境における偽造された記録を回避する。

出版業者のＰＣＭＣＩＡカード３３に記憶された監査情報は、課金／アクセスセンタによって監査可能である。課金／アクセスセンタと出版業者との間に伝送ラインがあることから、課金／アクセスセンタは、出版業者のＰＣＭＣＩＡカード３３に記憶された情報にアクセスし、システムを利用することを含む多くの目的に対する出版業者の動きを分析することができる。

ＰＣＭＣＩＡカード３３を、ハードウエアカード、またはハードウエアカード

をエミュレートするソフトウエアアプリケーションとすることができる。標準的な特徴として、揮発メモリまたはＲＡＭ４６およびバスインタフェース４７を含み、出版業者のコンピュータシステム３６と通信できるようにする。

出版業者が、実際に何らかの情報をＣＤ－ＲＯＭに対して暗号化および／または署名できるようになる前に、キーボードインタフェースまたは、カード読み取り器に直接入力することができるものによるログオンフレーズをサポートするＰＣＭＣＩＡカード３３にログを記入する。このフレーズを、出版業者が割り当てるいかなる長さにしてもよく、いかなるアスキー文字列にしてもよい。セキュリティの強化のために、出版業者は、出版業者をカードおよびその資源に結合するより安全なログオンのために、ログオンフレーズの後に生物測定（声）を使用してもよい。出版業者は、何らかのセキュリティに関係する機能を行う前に、カードにログを記入する。

ログオンの後、出版業者は、ＰＣＭＣＩＡカード３３の資源を使用することができる。出版業者のコンピュータ３６におけるソフトウエア機能か、別個のハードウエアカードとして実行されるカードは、電子出版サービスをサポートするＣＤを生成するために、出版業者によって必要な暗号化機能のすべてを提供する。ＣＤアプリケーションに対する暗号化を、セクタレベルにおいて行い、大きなデータベースにおけるランダムアクセスをサポートする。マイクロプロセッサ４８は、暗号化装置４３として動作し、出版業者が、ファイル、ディレクトリ、サブディレクトリ、ボリューム、または媒体全体を、個々の対称暗号化鍵と関係付けられるようにし、暗号化を実行するのに使用される。署名および鍵交換アルゴリズムを、選択された人格によって決定される公開／非公開鍵を使用して行う。これらのアルゴリズムを、構成可能性のためにソフトウエアにおけるものとするが、マイクロプロセッサにおけるハードウエアに実装してもよい。マイクロプロセッサを、すぐ入手できるマイクロプロセッサとすることができる。ＰＣＭＣＩＡカード３３は、有限状態機械として動作する。出版業者のアプリケーションは、遠隔地の課金／アクセスセンタに戻す鍵属性規定の同期化に従う。

図７のフローチャートは、本発明の一連のステップを説明し、これらの大部分は、上記において詳述した。プログラム開始５１の後、ステップ５２において、

データを、ＣＤ－ＲＯＭにおいて出版すべきデータセットに編成する。ステップ５３において、各々のデータセットに関する課金構造を準備する。次に、別々の属性を、データセットに関係付ける。例えば、判定ボックス５４に従って継続期間を割り当てる場合、ステップ５６においてタイムベースを設定し、属性をデータセットに関係させる。または、アクセスのバイト数を、データセットに判定ボックス５７に従って割り当て、次にステップ５８において、このバイト数および属性を、データセットに関係させることができる。または、特定の処理を、出版業者によって規定し、判定ボックス５９および６１にしたがって設定し、次にデータセットに関係させることができる。属性を生成し、関係付けた後、ステップ６２において、新たな鍵を、鍵データベース４２から得る。次にこのデータを、暗号化のために準備する。ステップ６３において、このデータを暗号化する。ステップ６４において、鍵セクタおよび署名表を構成する。ステップ６６において、次のデータセットに関する完全な処理を繰り返す。全てのデータを処理した場合、ステップ６７において、鍵セクタおよび署名表をＣＤに書き込み、出版業者に供給し、出版業者自身の記録と課金／アクセスセンタデータベースの記録とを更新する。

図８および９は、プログラムを出版業者に提供する方法の１つを説明する。このユーザフレンドリインタフェースによって、出版業者は、属性を割り当てる部品をポイントし、クリックし、ドラッグする。出版業者は、暗号化すべき同様のアプリケーションを、同じ暗号化鍵グループ６８によって組分けすることができる。出版業者が、個々のデータセットの一部の暗号化を望まない場合、出版業者は、バイパスステップ６９を選択し、ファイルに関係するハイパテキストまたはキーワード検索を暗号化しないようにすることができる。これは、購読者が、データベースを購入する前に、個々のワードまたは処理の付随するものの数を決定したい場合、特に有用である。

出版業者が、鍵グループの関係付けと暗号化のレベルを決定した後、出版業者に、鍵グループに対する課金属性を規定するメニューの第２の組を提供する。図９は、鍵グループに対するセキュリティデフォルトを設定するためにユーザに提供されるインタフェースの形式の一例である。これらは、ユーザアクセス日数、

月数または年数の連続ユニットと、ユーザが規定したアプリケーションの鍵開始日と、鍵の終了と、ユーザアクセス分、時または日の合計時間と、伝送されたバイト、ワードまたはユーザが規定した処理の合計ユニットと、ユーザのログオンの合計とを含むが、これらに限定されない。鍵別名を、より簡単な鍵確認のために規定することができる。

これらのオプションは、新たな（使用されていない）鍵、またはすでに別名が付けられている（使用されている）鍵において利用可能である。出版業者か、これらの属性を規定した後、前マスタリングソフトウエアは、出版業者鍵データベースを、これらのパラメータによって更新する。出版業者は、存在している鍵を使用するので、出版業者は、この鍵に暗号化更新処理を用いるオプションを有する。この処理を、既知の定数を使用し、この定数を（排他的にまたは関数によって）古い鍵に数学的に用いることによって規定する。

全ての更新を、鍵に関係付けられた鍵カウンタによって保持する。これによって、出版業者および購読者は、出版された材料と同期した月１回出版される鍵および更新カウンタを保持することができる。予約講読アクセスを、購読者によって購入された期間、許可された更新数によって制御する。

鍵マネージャまたはデータベース４２（図５参照）は、出版業者によって製造された個々のＣＤ－ＲＯＭに使用されたＫＭＩＤの監査／履歴ファイルを保持する。ＣＤ－ＲＯＭが製造された後、鍵マネージャ４２は、自動的に出版業者の課金／アクセスセンタを呼び、構成された属性情報をダウンロードする。

ＣＤ－ＲＯＭは、関係するＫＭＩＤに対するセクタの開始および終了についての情報を含む。この情報を、ＣＤ－ＲＯＭのどこにでも配置することができる別個の表において保持する。図１０は、このような表を示す。出版業者のディジタル署名ファイル７０ａは、署名データファイル７０ｂを含む。出版社の情報７０ｃと、暗号化アルゴリズム情報７０ｄと、更新アルゴリズム情報７０ｅと、出版しているデータに関連する広告情報７０ｆと、鍵セクタおよび署名表７０ｇを含む上述した他のファイルも、ＣＤ－ＲＯＭに含める。

鍵セクタおよび署名表７０ｇは、この媒体の形成にににおいて使用されたＫＭＩＤについての情報を含む。最も重要に、この表は、使用されたＫＭＩＤに対する

セクタの停止および開始を含む。

図１１に戻ると、図２に示す特徴の多くを再び示すが、ブロック図形式において示す。しかしながら、監査／復号化装置および呼出しアプリケーション７１を、ユーザのコンピュータ３１と区別する。この装置を、ユーザのＰＣＭＣＩＡカード２９におけるものとするか、別個のハードウエア、またはユーザのコンピュータ３１にインストールされたソフトウエアとすることができる。

ユーザのＰＣＭＣＩＡカード２９は、標準的なバスインタフェース７２およびＲＡＭ７３を含む。不揮発性メモリは、人格および監査機能のような、上述したこのような特徴を含む。マイクロプロセッサ７６は、暗号化／復号化、署名、鍵交換アルゴリズムを含む。

ユーザのＰＣＭＣＩＡカード２９における特徴のユーザによる操作を、図１３のフローチャートにおいて示す。一連の事象の開始７７の後、ステップ７８において、ユーザは、定期的に流通される媒体を得る予約講読サービスを注文する。ステップ７９において、ユーザは、例えば郵便によってＣＤ－ＲＯＭを得て、カードおよびＣＤ－ＲＯＭをロードする。ユーザのコンピュータ画面において、ユーザは、図１０に示したのと同様の、ＣＤ－ＲＯＭに記憶された情報を閲覧する。ステップ８１において、ユーザは、鍵に対する電子メール要求を発生および署名し、課金／アクセスセンタに送る。ステップ８２において、認証および許可を行った後、ユーザは、鍵を電子メールを経て課金／アクセスセンタから得る。ステップ８３において、鍵を、ユーザのＰＣＭＣＩＡカード２９に記憶する。さらにカードは、構成された属性に従ってユーザの活動の監査ログを保持する。この監査に、課金／アクセスセンタは、いくつかの目的の使用を監視するために、遠隔的にアクセスすることができる。例えば、この使用を監査し、予約講読が出版された後、ユーザが何回同じ出版物を閲覧したかについての情報を、出版業者に提供する。最後に、ステップ８４において、ユーザは、選択したファイルにアクセスする。

図１４を参照すると、課金／アクセスセンタ２３の特徴を、ブロック図に示す。すでに上述した特徴は、ユーザおよび出版業者の双方に対するリモートリンク２７を含む。大容量鍵データベースは８５は、出版業者に分配すべき鍵を、デー

タの暗号化において使用するために保持する。購読者データベース８６は、すべての購読者のリストと、購読者のシステムの使用の前または後に、または監査によって得られる購読者についての特定の情報とを含む。出版業者データベース８７は、鍵およびこれらに関係するＫＭＩＤの出版業者の使用を含む。掲示板８８は、購読者および出版業者から来るメッセージを保持する。システムの新しい特徴または他の情報を通知するメッセージを、購読者および出版業者の双方に送ることもできる。

課金／アクセスセンタは、出版業者から来る要求に対する掲示板の登録または呼出しが来ることによって開始８９を処理する。ステップ９２において、課金／アクセスセンタは、電子要求を読み、メッセージの電子署名を照合することによって購読者を認証する。ステップ９３において、要求によって供給されたＫＭＩＤから、属性を一致させ、課金情報を提供する。任意に、ステップ９４において、課金／アクセスセンタは、ユーザと通信し、ＣＤ－ＲＯＭメニューに示されていない時間支払いまたは申込みのような課金オプションを、ユーザに提供することができる。ステップ９５において、課金を清算する場合、課金／アクセスセンタは、購読者の支払い方法を確認し、ユーザからの購入申込みを受ける。署名または支払い方法が満足されない場合、課金／アクセスセンタは、ステップ９６において、鍵およびログの試みを拒絶する。これらが満足された場合、ステップ９７において、鍵をユーザのＰＣＭＣＩＡカード２９にダウンロードする。ステップ９８において、課金／アクセスセンタは、さらなる要求に関して質問する。さらなる要求が無い場合、監査ファイルをダウンロードし、ステップ９９においてカードから現在のユーザＫＭＩＤ監査ファイルを得て、各々ステップ１００および１０１において、購読者データベース９７を更新し、出版業者の勘定書を更新する。ステップ９８の質問に対する答えがイエスなら、システムは、ステップ９３に戻り、異なったデータファイルおよびＫＭＩＤに関して、処理を再び開始する。

課金／アクセスセンタのユーザとの通信を、上述したインタラクティブなものとすることができ、または、要求が送信され、これが許可または拒絶されるように構成することもできる。何らかの事象において、課金／アクセスセンタは、Ｋ

ＭＩＤを受け、許可が成された場合、鍵をユーザに送り、ＣＤ－ＲＯＭに記憶されたデータへのアクセスをする。

簡単に上述したように、暗号化更新処理は、古くなった情報または購読者の継続期間を過ぎて発売された出版物へのアクセスを防ぐ方法を提供する。暗号化更新処理を、属性データ構造におけるさらに他のフラグとする。月刊または隔週刊雑誌の出版業者は、多くの情報を定期的に極めて長い継続期間（年）とすることができる間、出版する。雑誌の出版業者は、このデータを受ける彼らのサービスに対する購読者を有する。購読者は、彼らの予約講読サービスがオンラインである継続期間の間、有効である鍵に結合し、これによってダウンロードする。しかしながら、これによって、出版物の流通期間中すべての暗号化に同じ鍵が使用される場合、出版業者は、大変攻撃されやすい状態におかれる。遠隔的な暗号化更新処理の目的は、雑誌の出版業者が、各月毎に購読者の現在の組に対して新たな鍵をダウンロードする必要なしに、異なった暗号化鍵に属する各々の雑誌を送ることができるようにすることである。

理想的には、出版業者は、各月毎に異なった鍵に従って暗号化された情報を流通させる。このようにすることは、出版業者の情報を、彼らの鍵を決定し、彼らの出版物のすべてを得る外部の攻撃者から保護する。しかしながら、これは、例えば購読者が、各月毎に新たな鍵をダウンロードする必要があることを意味する。これは、購読者にとって、極めて煩わしいものとなるであろう。本発明によるシステムは、現在の（または毎月の）鍵に用い、現在の月の鍵に基づいて新たな鍵を「発生」する、ユーザサイト暗号化更新の使用を規定する。すべてのカードは、更新処理に使用すべきアルゴリズムを理解することから、これらは、同じ鍵値を得る。出版業者は、このアルゴリズムを知り、これを使用して、暗号化処理のための更新鍵値を発生する。出版業者が、材料を毎月生産する場合、各々の新たな出版物のための鍵における「更新」を毎月行う。購読者が、新たなＣＤ－ＲＯＭを得た場合、ＣＤ－ＲＯＭの更新カウンタが、更新が何回行われたかを、ユーザのＰＣＭＣＩＡカードに通知する。更新カウンタを使用し、出版業者および購読者間の同時性を保持する。

例えば、図１６に戻ると、ある年の予約講読サービス期間が示されている。１

２か月を、列において関係させる。各月は、列１０７において示されるように関係付けられたK_A、K_B等として示すような異なった鍵を有する。列１０８において示す「購読者１」を、この年の第２の月において開始する６か月の予約講読を有するものとして示す。「購読者１」は、鍵K_Bを受け、第２の月において発行されたデータにアクセスする。上述したような更新処理は、鍵K_Bを数学的な演算によって更新し、ここで更新処理Ｕは、前の月の鍵に作用する。例えば、ＵがK_Bに作用すると、$K_C = UK_B$となる。さらに、予約講読の第３の月にＣＤが利用可能になると、ＵがK_Bに作用し、$K_D = UK_C = UUK_B$となる。K_DからK_Gが、同様に発生する。したがって、本発明の暗号化更新処理によって、「購読者１」は、月２から月７の間の発行物へのアクセスを行う鍵の組を受ける。列１０９に示す別の購読者「購読者２」は、同じく６か月の予約講読を有しているが、それは第４の月から始まり、鍵K_Dを受ける。本発明の更新処理は、鍵K_Dを更新し、ＵがK_Dに作用し、$K_E = UK_D$となる。さらに、予約講読の第３の月にＣＤが利用可能になった場合、ＵがK_Eに作用し、$K_F = UK_E = UUK_D$となる。K_GからK_Iが、同様に発生する。したがって、「購読者１」および「購読者２」は、部分的に重なった異なった継続期間中の予約講読を有している間、更新処理によって、重なっている月のアクセスに同じ鍵を使用する。この年の発行物のある部分へアクセスするために、毎月の更新によって、最初にダウンロードした鍵からアクセス符号を発生する処理は、出版業者が、異なった時に開始し、異なった継続期間を有する予約講読サービスを、許可されたサービスより多くのデータへのアクセスを与えることなしに提供することを可能にする。ＫＭＩＤパラメータは、購入された更新の回数を規定する。図１６の例において、ＫＭＩＤは、各々のユーザに対して５回の更新を規定する。

したがって、本発明は、ユーザによって使用されるデータ検索システムを含み、このシステムは、複数のＣＤ－ＲＯＭのような小型データ記憶媒体を含み、本システムにおいて、例えば逐次的に発行されたある出版物の各々が、複数のＣＤ－ＲＯＭのあるものに記憶されたデータを含む。ＣＤ－ＲＯＭにおけるデータの一部を、アクセス符号の大きな組（すなわち、K_AからK_L）の一部であるアクセス符号の組（すなわち、K_BからK_G）によってアクセス可能なユーザによっ

て選択し、ここで、アクセス符号の組のあるものは、課金／アクセスセンタによってユーザに伝送されたような、伝送されたアクセス符号である。複数のＣＤ－ＲＯＭの以前アクセスできなかったものにアクセスするために、これらのＣＤ－ＲＯＭは、伝送されたアクセス符号に協調的な、複数のＣＤ－ＲＯＭの他のものにおけるデータにアクセスするためのアクセス符号を更新する符号を含む。

更新処理は、現在の鍵（月々の出版物において使用されるもの）を使用する。この鍵に対して、固定された既知の定数を数学的に用い、例えば、現在の鍵に排他的論理和する。この数学的演算から結果として生じる値を、次の出版物に対する復号化鍵として使用する。更新属性を有するすべての鍵を、これらの更新カウンタによって保持する。これによって、ユーザは、例え１つまたは２つの出版物を取り損なったとしても、これらの鍵を同期させることができる。この処理は、講読者のサイトにおいて生じる。出版業者は、同じ機能を行い、同じ値を用いて、新たな暗号化鍵を生成する。情報を、この新たな暗号化鍵によって暗号化する。暗号化されない暗号化情報および更新カウンタを、流通するＣＤ－ＲＯＭに記録する。

【図１】

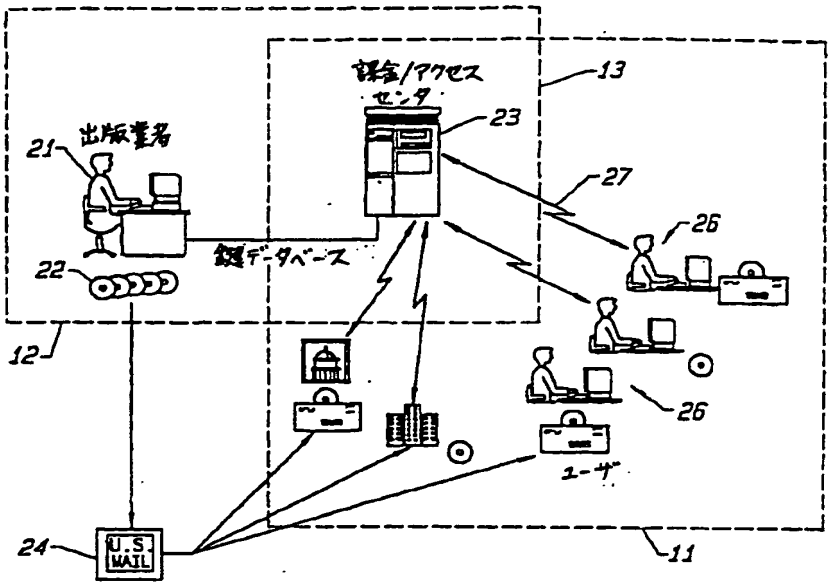


FIG. 1

【図２】

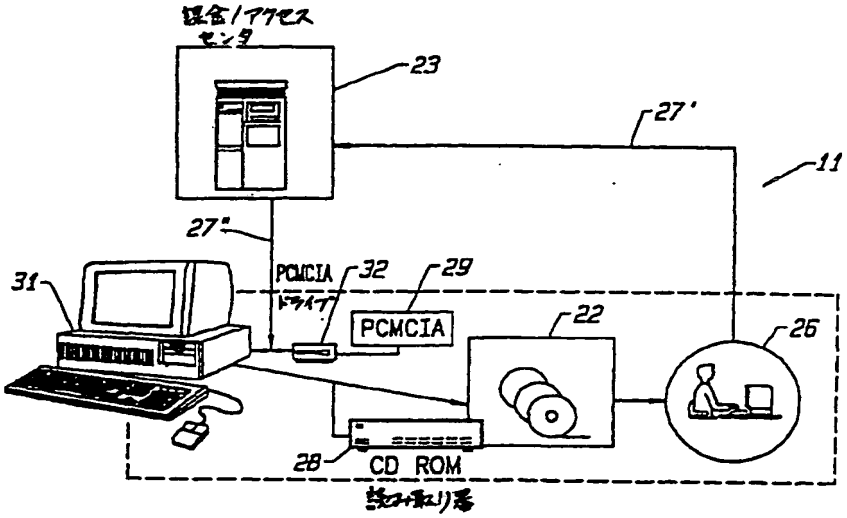


FIG. 2

【図３】

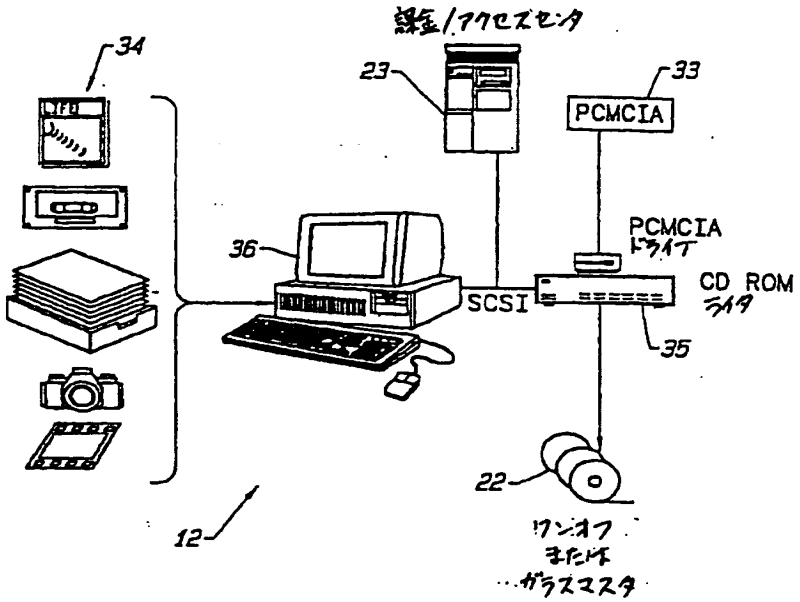


FIG. 3

【図４】

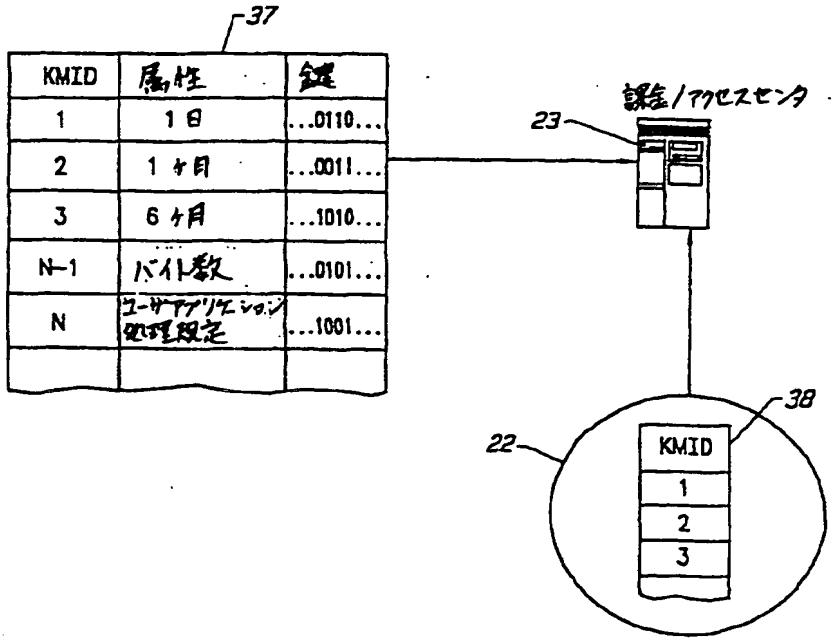


FIG. 4

【図５】

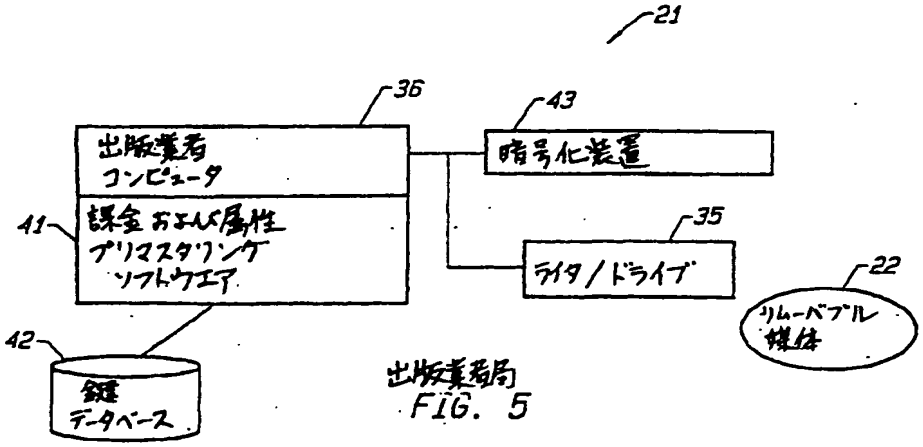
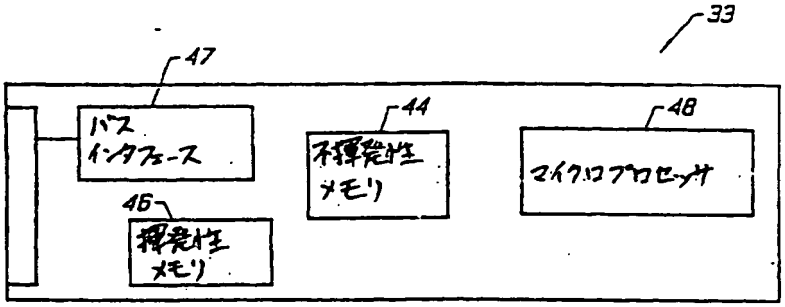


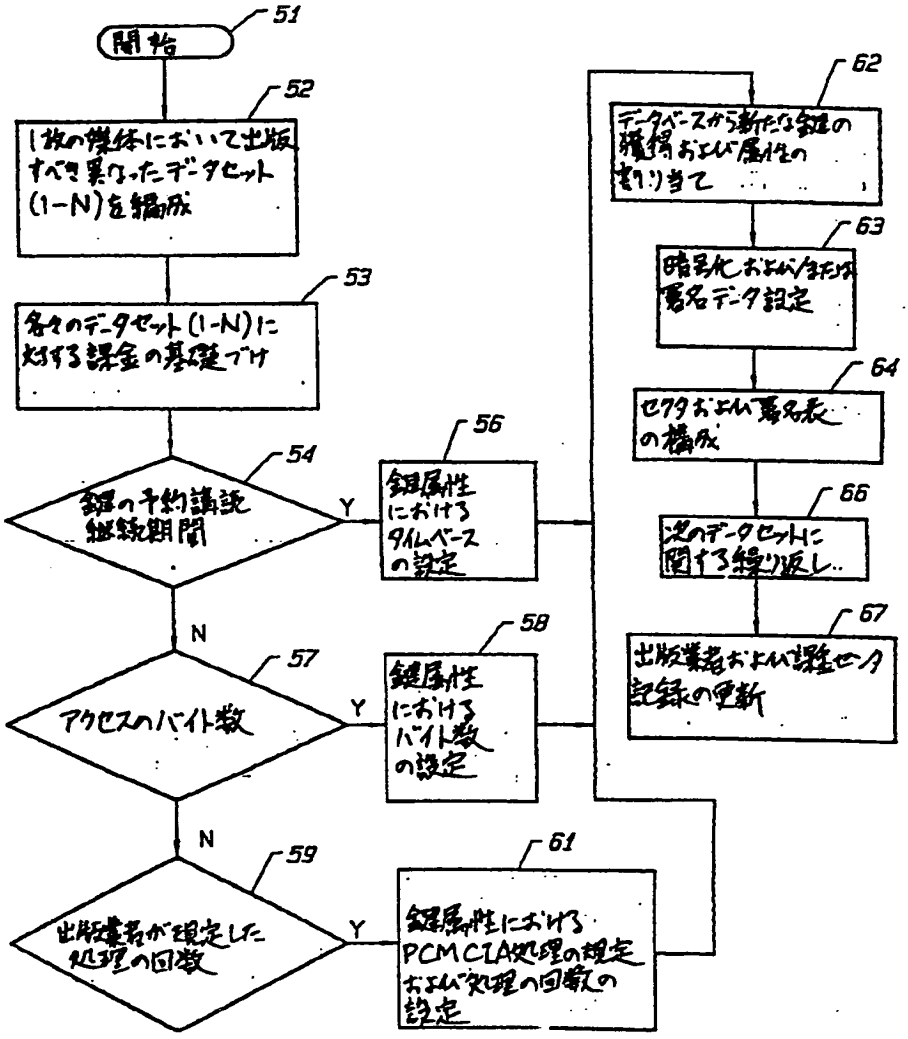
FIG. 5

【図６】



出版業者暗号化装置
FIG. 6

【図７】



出版業者の課金ソフトウエア

FIG. 7

【図８】

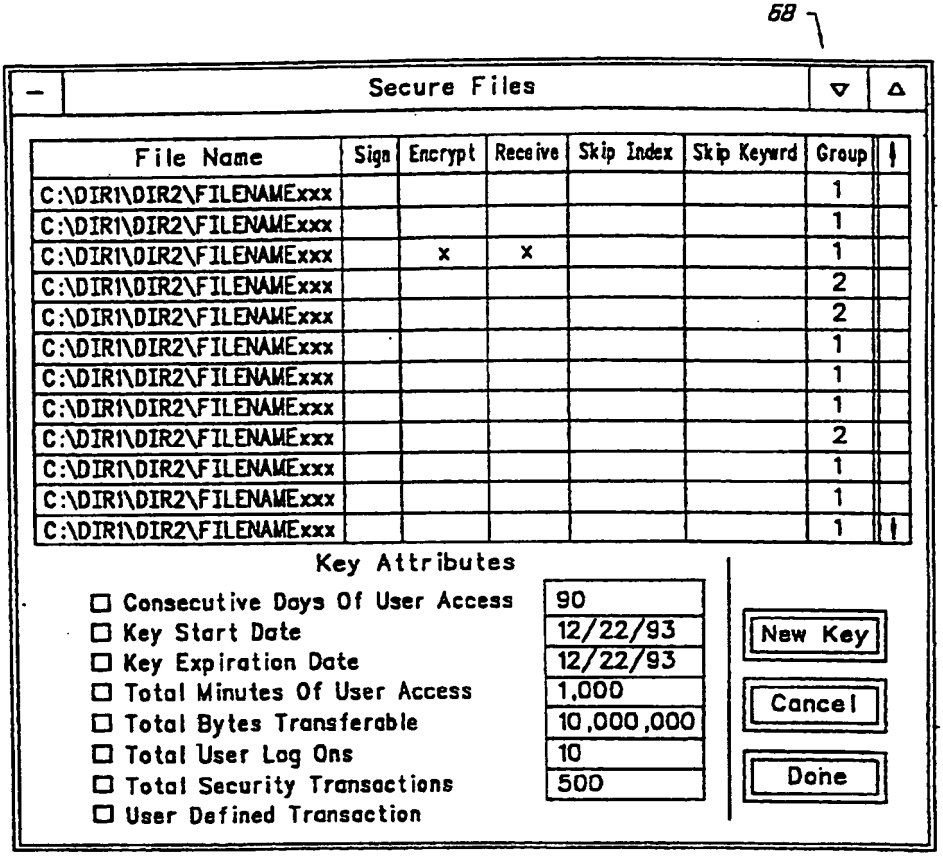

68
Secure Files
File Name
Sign
Encrypt
Receive
Skip Index
Skip Keywrd
Group
C:\DIR1\DIR2\FILENAMExxx
1
2
x
Key Attributes
Consecutive Days Of User Access
Key Start Date
Key Expiration Date
Total Minutes Of User Access
Total Bytes Transferable
Total User Log Ons
Total Security Transactions
User Defined Transaction
90
12/22/93
1,000
10,000,000
10
500
New Key
Cancel
Done

FIG. 8

【図９】

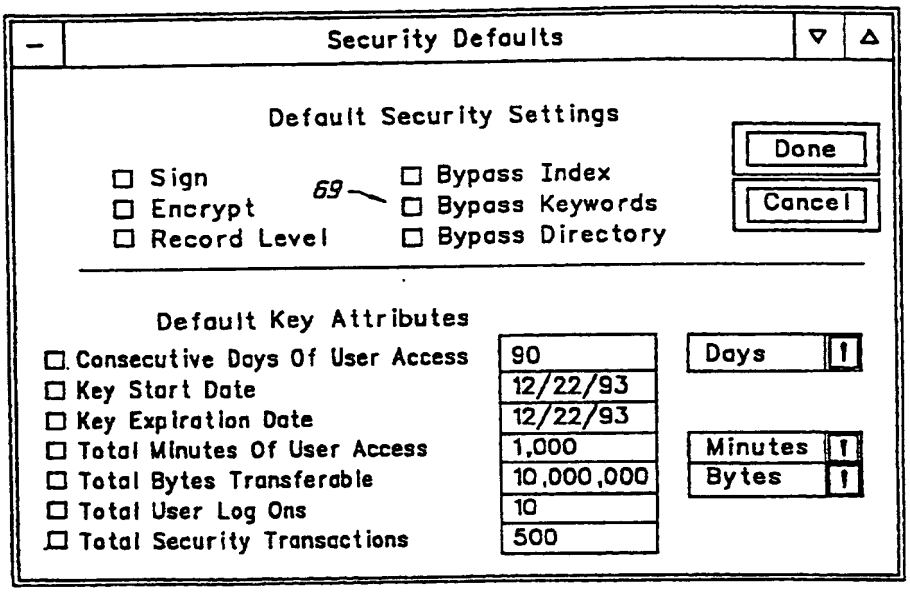

Security Defaults
Default Security Settings
Done
Cancel
Sign
Encrypt
Record Level
69
Bypass Index
Bypass Keywords
Bypass Directory
Default Key Attributes
Consecutive Days Of User Access
Key Start Date
Key Expiration Date
Total Minutes Of User Access
Total Bytes Transferable
Total User Log Ons
Total Security Transactions
90
12/22/93
12/22/93
1,000
10,000,000
10
500
Days
Minutes
Bytes

FIG. 9

【図１０】

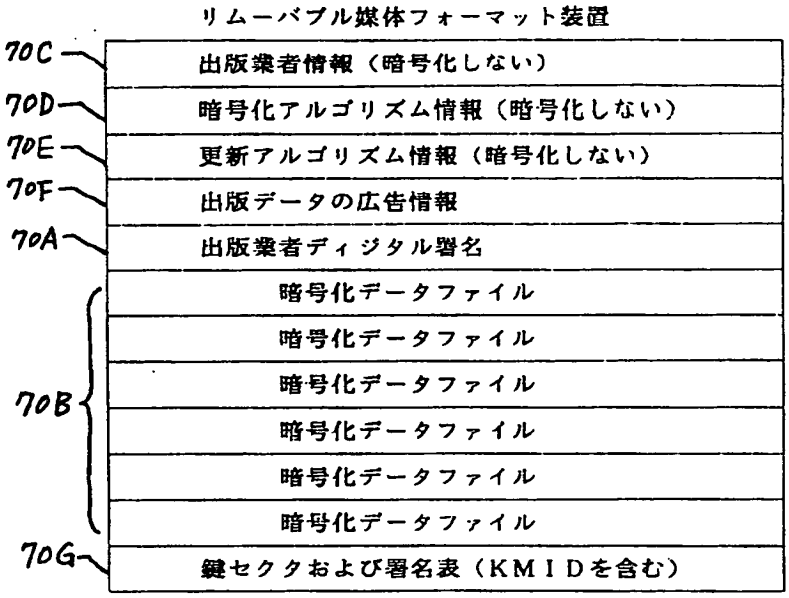


FIG. 10

【図１１】

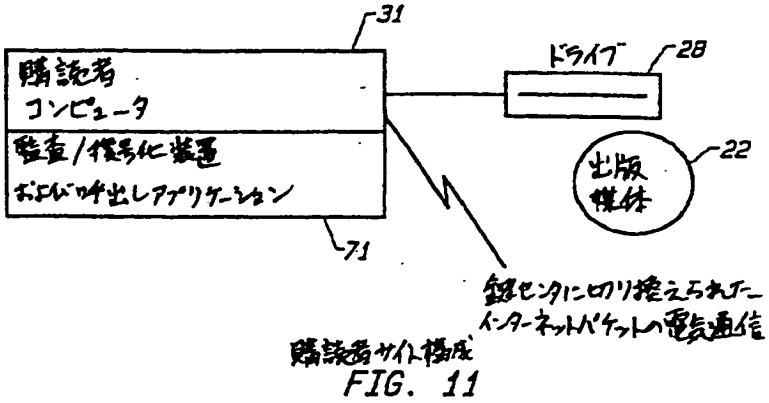
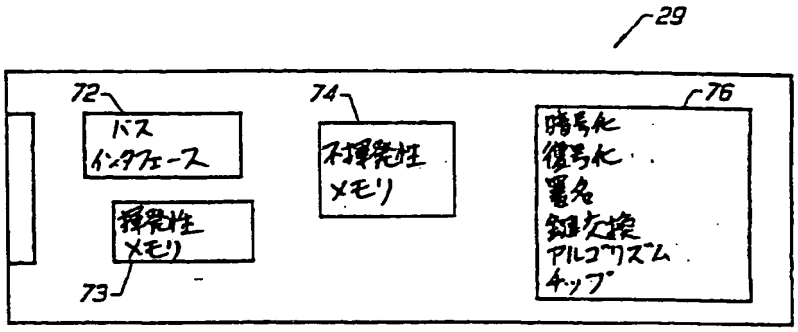


FIG. 11

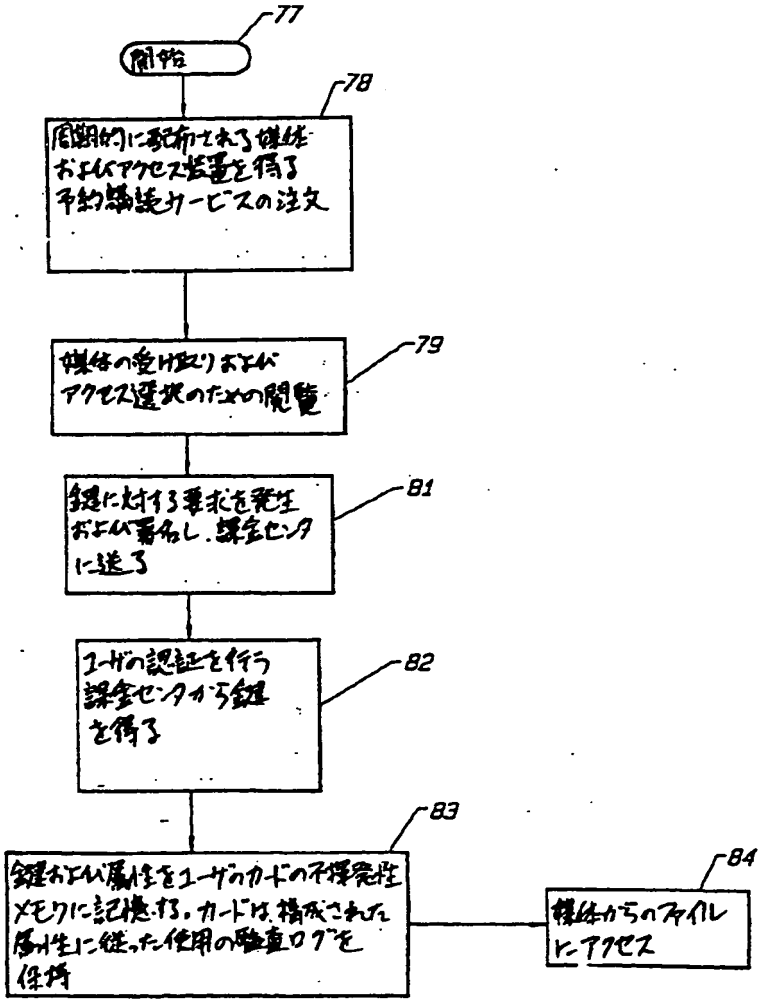
【図１２】



監査復号化装置

FIG. 12

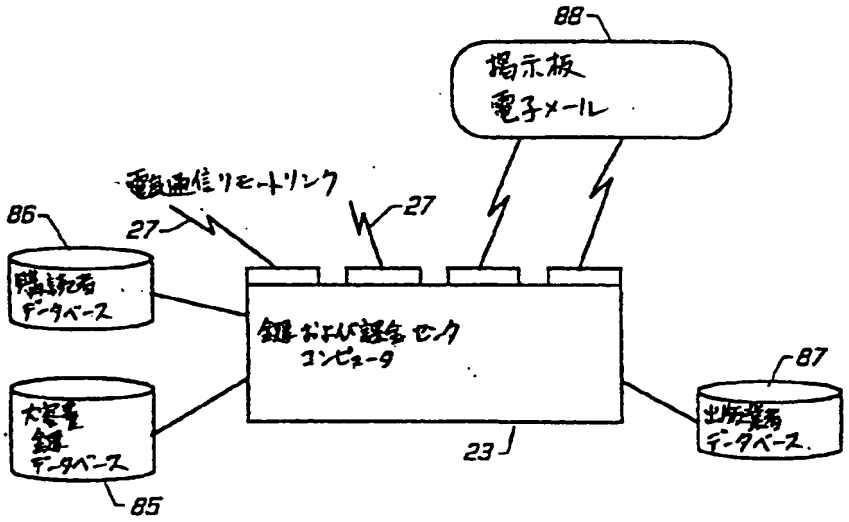
【図１３】



購読者鍵要求処理

FIG. 13

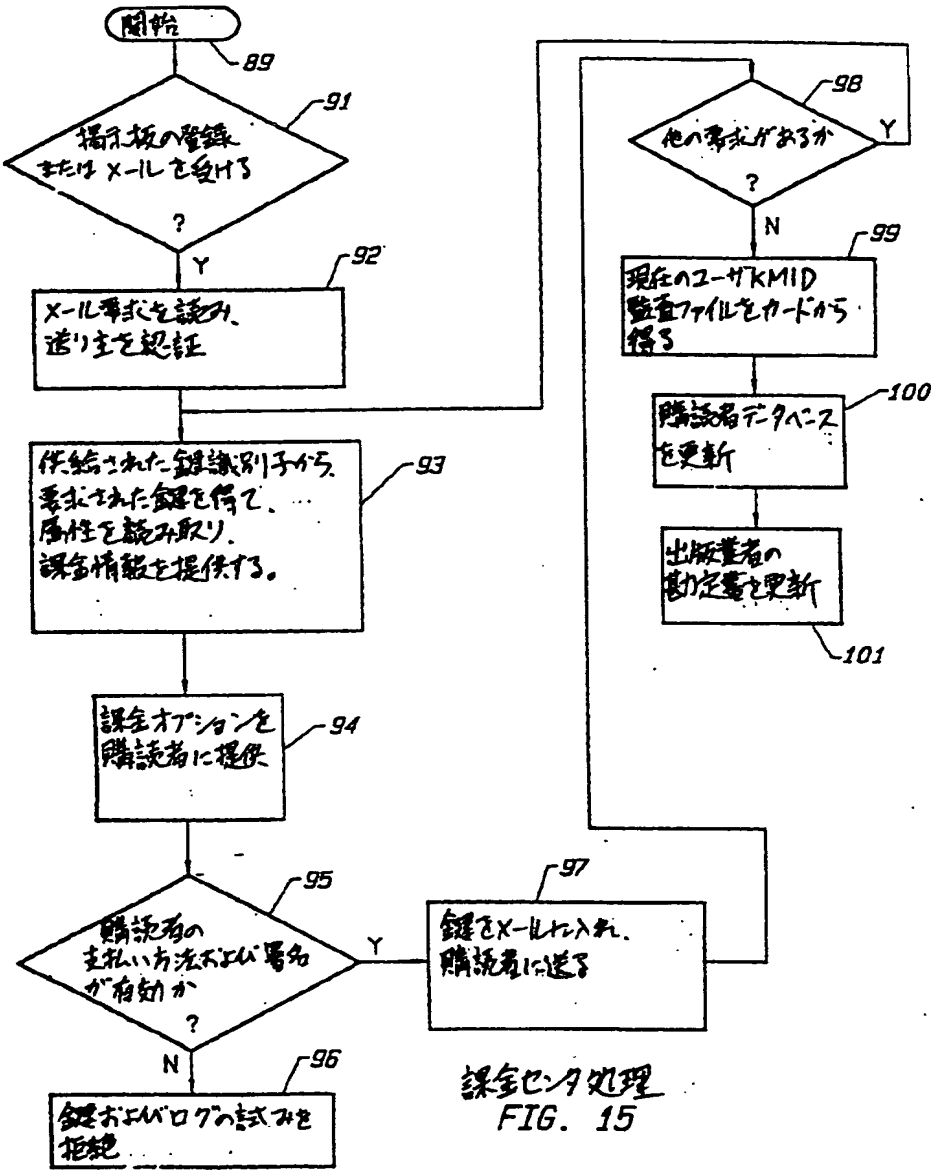
【図１４】



録音/アクセスセンタおよびデータベース

FIG. 14

【図１５】



課金センタ処理
FIG. 15

【図１６】

106 月	107 鍵	108 購読者１	109 購読者２
1	K_A		
2	$K_B=UK_A$	６ヶ月	
3	$K_C=K_B=UUK_A$		
4	$K_D=UK_C$		６ヶ月
5	$K_E=UK_D$		
6	$K_F=UK_E$		
7	$K_G=UK_F$		
8	$K_H=UK_G$		
9	$K_I=UK_H$		
10	$K_J=UK_I$		
11	$K_K=UK_J$		
12	$K_L=UK_K$		

例．ある年のサービス期間

FIG. 16

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/10455

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04K 1/00
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/25
380/22,23,24,28,29,30,49,50

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, A, 4,888,798 (EARNEST) 19 DECMEBER 1989. SEE FIGURE 2.	1-46
X	US, A, 4,827,508 (SHEAR) 02 MAY 1989 SEE FIGURE 4.	1-46

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 13 OCTOBER 1994	Date of mailing of the international search report DEC 13 1994
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer TOD R. SWANN Telephone No. (703) 308-0475

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

Int. ational application No.
PCT/US94/10455

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

380/25
380/22,23,24,28,29,30,49,50

フロントページの続き

(51)Int.Cl.6		識別記号	庁内整理番号	FI		
G09C	1/00	640	7259－5J	G09C	1/00	660D
		660	7736－5D	G11B	20/10	H
G11B	20/10		9180－5J	H04H	1/02	E
H04H	1/02		9570－5J	H04L	9/00	673A
H04L	9/32		9570－5J			673D
			7925－5L	G06F	15/21	Z

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, MW, SD), AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LT, LU, LV, MD, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, US, UZ, VN